REMARKS/ARGUMENTS

Claims 1-67 were pending in this application when last examined by the Examiner. Claims 3, 5-8, 11-20, 46, 48, 50-51, and 53-55 have been amended. Claims 1-2, 4, 9-10, 22-45, 47, 56-67 have been canceled. Claims 68-79 have been added. The amendments find full support in the original specification, claims, and drawings. No new matter has been added. In view of the above amendments and remarks that follow, reconsideration, reexamination, and an early indication of allowance of the now pending claims 3, 5-8, 11-20, 46, 48, 50-51, 53-55, and 68-79 are respectfully requested.

Claims 1-3, 5-12, 15, 17-21, 44-46, 48-49, 51-52, and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda et al. (U.S. Patent No. 6,769,063) in view of Callum (U.S. Patent No. 6,320,964), Kamishima (U.S. Patent No. 6,236,686) and Adler (U.S. Patent No. 4,255,811). Applicant respectfully traverses this rejection.

Independent claims 1 and 44 have been canceled in favor of new claims 68 and 73. Accordingly, the rejection of claims 1 and 44 will be addressed with reference to claims 68 and 73.

Applicant respectfully submits that neither Kanda, Callum, Kamishima, nor Adler teach or suggest all the limitations of claims 68 and 73. Kanda discloses in column 2, lines 22-38, and in FIG. 2, a conventional DES cryptographic device that includes an expansion unit (reference 17) that takes a first 32-bit block data Ri and provides a 48-bit expanded data to an XOR circuit (reference 18). The XOR circuit exclusive ORs the expanded data with a subkey. The output of the XOR circuit is fed to eight S-boxes which together generate a 32-bit output from the 48-bit input. A permutation part (reference 19) takes the output of the S boxes and provides a permuted output. This permuted output is then exclusive ORed with a second 32-bit block data Li.

The drawback of such a conventional cryptographic device is described in Applicant's application. Specifically, such a conventional cryptographic device cannot support a bit-sliced implementation because the permutation part (reference 19) and expansion unit (reference 17) change the order of bits in the 32-bit block data Ri. (Specification p. 16, lines 29-31). To solve

this problem, the claimed cryptography engine includes "an inverse permutation logic performing an inverse permutation of a bit sequence associated with the second portion of the data block and generating an inverse permuted bit sequence; means for combining via a second logical operation the second bit sequence with the inverse permuted bit sequence and generating a combined bit sequence; and a permutation logic permuting the combined bit sequence and generating a permuted bit sequence." (Emphasis added). These limitations are not taught nor suggested by Kanda.

Callum discloses a cryptographic accelerator that includes a selector and a plurality of buses coupled to the selector. In Callum, "[t]he buses include signal lines for performing an initial permutation, various complex key-dependent computations, and an inverse of the initial permutation." (Col. 4, lines 10-13). Callum also teaches a permutation operation permuting the bits of an input data block. (Col. 6, lines 11-14). Nothing in Callum teaches or suggests that the disclosed inverse of the initial permutation engages in "performing an inverse permutation of a bit sequence associated with the second portion of the data block and generating an inverse permuted bit sequence," nor that the initial permutation or permutation operation engages in "permuting the combined bit sequence and generating a permuted bit sequence," where the combined bit sequence is a result of "combining via a second logical operation the second bit sequence with the inverse permuted bit sequence." (Emphasis added).

Adler discloses a cryptographic system that includes permutation blocks 22 and 32 which are inverse of each other. (Col. 5, lines 33-34). However, there is no teaching or suggestion that permutation block 32 engages in "performing an inverse permutation of a bit sequence associated with the second portion of the data block and generating an inverse permuted bit sequence." (Emphasis added). Furthermore, there is no teaching or suggestion that permutation block 22 engages in "permuting the combined bit sequence and generating a permuted bit sequence," where the combined bit sequence is a result of "combining via a second logical operation the second bit sequence with the inverse permuted bit sequence." (Emphasis added). Accordingly, independent claims 68 and 73 are now in condition for allowance.

Claims 2, 9-10, and 45 have been canceled.

Claims 3, 5-8, 11-12, 15, 17-21, 46, 48-49, 51-52, and 55 are also in condition for allowance because they depend on an allowable base claim and for the additional limitations that they contain.

Claims 4, 13-14, 47, and 53-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda in view of Callum, Kamishima, and Adler, and further in view of Steinman (U.S. Patent No. 6,591,349).

Claims 4 and 47 have been canceled. Claims 13-14 and 53-54 are in condition for allowance because they depend on an allowable base claim, and for the additional limitations that they contain.

Claims 16 and 50 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda in view of Callum, Kamishima, Adler, and Steinman, and further in view of Teppler (U.S. Patent No. 6,792,536). Claims 16 and 50 are in condition for allowance because they depend on an allowable base claim, and for the additional limitations that they contain.

Claims 22-24, 26-33, 35-40, 43, 56-58, 60-61 63-64, and 67 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda in view of Callum. Claims 25, 41-42, 59, and 65-66 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda in view of Callum and in further view of Steinman. Claims 34 and 62 are rejected under 35 U.S.C. 103(a) as being unpatentable over Kanda in view of Callum and Steinman and in further view of Teppler. Claims 22-43 and 56-67 have now been canceled. Withdrawal of the rejection with respect to these claims is respectfully requested.

Claims 69-72 and 74-79 are new in this application. Claims 69-72 and 74-77 are in condition for allowance because they depend on an allowable base claim, and for the additional limitations that they contain.

New claim 78 recites a "cryptography engine for performing cryptographic operations on a data block, the cryptography engine comprising: a key scheduler configured to provide keys for cryptographic operations; an expansion logic expanding a bit sequence associated with the first portion of the data block and generating an expanded bit sequence having a first bit size; a first XOR logic performing a first XOR operation of a first key provided by the key scheduler and the

expanded bit sequence and generating a first combined bit sequence; an Sbox logic taking the first combined bit sequence and generating a second bit sequence having a second bit size smaller than the first bit size; an inverse permutation logic performing an inverse permutation of a bit sequence associated with the second portion of the data block and generating an inversed permuted bit sequence; a second XOR logic performing a second XOR operation of the second bit sequence and the inverse permuted bit sequence and generating a second combined bit sequence; and a permutation logic permuting the second combined bit sequence and generating a permuted bit sequence." For the reasons discussed above with respect to claims 68 and 73, neither Kanda, Callum, nor Adler, alone or in combination, teach or suggest all of the limitations of new claim 78. Accordingly, claim 78 is also in condition for allowance.

New claim 79 is also in condition for allowance because it depends on an allowable base claim, and for the additional limitation that it contains.

In view of the above amendments and remarks, Applicant respectfully requests reconsideration, reexamination, and an early indication of allowance of the now-pending claims 3, 5-8, 11-20, 46, 48, 50-51, 53-55, and 68-79.

Respectfully submitted,
CHRISTIE, PARKER & HALE, LLP

By _____
Josephine E. Chang
Reg. No. 46,083
626/795-9900

JEC/lal
AB PAS647657.2-*-11/29/05 1:05 PM